GDPR - PERSONVERN

Advokat Sunniva Berntsen

Hvorfor personvern?

Viktig i et demokratisk samfunn

EMK artikkel 8

Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.

Grunnloven § 102

Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.

Personvernforordningen
GDPR Regulation (EU) 2016/679

Bakgrunn

- Felles regelverk i Europa
- Styrke den europeiske borgers rettigheter
- Gjøre det lettere å utveksle personopplysninger over landegrenser
- Styrke tilliten til digitale tjenester
- Sikre samarbeid mellom personvernmyndigheter

Nye personvernregler fra 25.5.2018

- EUs personvernforordning trer i kraft 25. mai 2018

- Forslag om ny personopplysningslov - i kraft fra 25. mai 2018 – som implementerer EUs personvernforordning i sin helhet

Sanksjoner ved overtredelse

- Store bøter ved overtredelse av bestemmelsene
- 10 mill euro / 2 prosent av global omsetning – høyeste beløp av de to
- 20 mill euro / 4 prosent av global omsetning – høyeste beløp av de to
- Avhengig av forsømmelsen

Snart er 25. mai 2018 her…

Så sett i gang!

Videre gjennomgang

- Ord og uttrykk du må kjenne
- Grunnleggende krav til behandling av personopplysninger
- Hovedtrekk i nytt regelverk
- Veiledere

Ord og utrykk du må kjenne
Hva er personopplysninger?

Peder Ås
Lillevikveien 4
Lillevik
Fødselsnummer 161079 34573

Ord og uttrykk du må kjenne

- **Behandling av personopplysninger**

Ord og uttrykk du må kjenne
Sensitive personopplysninger

Kravet til behandlingsgrunnlag øker

- **Sensitiv personopplysning** – opplysninger om for eksempel genetiske og biometriske opplysninger, helse, seksuell legning, fagforeningstilknytning

- *Egen sensitiv kategori* - at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling.

Ord og uttrykk du må kjenne

- **Behandlingsansvarlig** – den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes (hovedansvarlig for at loven etterleves)
- **Databehandler** - den som behandler personopplysninger på vegne av en behandlingsansvarlig
- **Databehandleravtale -** En avtale mellom databehandler og behandlingsansvarlig om hvordan personopplysninger skal behandles.

Ord og uttrykk du må kjenne

- **Den registrerte** - den fysiske person som en personopplysning kyttes til
- **Personvernstrategi** – Beslutninger og tiltak for etterlevelse av personvernforordningen og ny personopplysningslov.
- **Internkontroll** – rutiner og tiltak for å overholde personvernregelverket

Grunnleggende krav til behandling av personopplysninger

- **Lovlighet:** behandlingen av personopplysninger må ha et rettslig grunnlag (også kalt behandlingsgrunnlag)
- **Rettferdighet:** forholdsmessighet mellom inngrepet og formålet
- **Gjennomsiktighet:** informasjonsplikter og innsynsretter

Grunnleggende krav til behandling av personopplysninger

- **Formålsbegrensning**: Formålet med registreringen skal være bestemt på forhånd, og opplysningene skal skal som hovedregel ikke benyttes til nye formål.
- **Data minimering:**
- De registrerte opplysningene skal dekke formålet, men ikke være mer omfattende

- **Riktighet**: Opplysningene skal være korrekte og oppdaterte

Grunnleggende krav til behandling av personopplysninger

- **Lagringsbegrensning:** Opplysningene skal anonymiseres eller slettes når behandlingen ikke er nødvendig for å nå formålet

- **Lagring og bruk av opplysningene på en så sikker måte at de ikke blir misbrukt**

- **Virksomheten er ansvarlig for, og skal kunne vise, at de grunnleggende kravene overholdes**

Krav til dokumentasjon for at reglene i forordningen overholdes

- **Internt dokument** som beskriver:

- hvilke typer av registrerte personer det er snakk om (for eksempel ansatte eller kontaktpersoner hos kunder)
- hva slags typer personopplysninger man behandler om dem (for eksempel navn, bankkontonummer, inntekt eller epostadresse)
- formålet med behandlingen (for eksempel administrasjon av ansatte eller å informere kunder om nye produkter)
- hva slags behandling man driver med (for eksempel innsending av opplysninger om ansattes inntekt til skattemyndighetene eller lagring av epostadresser)
- hvilke grunnlag man har for å behandle opplysningene (for eksempel legitim interesse, samtykke, lovforpliktelse eller avtale)
- at bedriften skal ha en personvernerklæring e.l.

Forpliktelser overfor de registrerte

- Retten til å bli glemt (sletting)
- Rett til å få utlevert opplysninger og til å få dem overført
- Opplysningsplikt om registrering og den registrertes rettigheter

Norske særregler på arbeidsrettens område

- Kameraovervåking på arbeidsplass og bruk av uekte kameraovervåkingsutstyr

- Regler om arbeidsgivers innsyn i e-postkasse mv.

Overføring utenfor EU/EØS

- Tredjeland som Kommisjonen har godkjent
- EU-US Privacy Shield
- Andre grunnlag for overføring til tredjeland:
  - Bindende virksomhetsregler
  - Standard personvernbestemmelser/-kontrakter
  - Den behandlingsansvarlige eller databehandleren gir nødvendige garantier og de registrerte har håndhevbare rettigheter
  - Unntaksvis - samtykke

Innebygd personvern i IKT-løsninger

- Krav til innebygd personvern i IKT løsninger
- Tekniske og organisatoriske tiltak
- For å ivareta personvernprinsipper
  - minimalisering
- Det minst personverninngripende alternativet som standard:
- En systematisk prosess

Databehandler direkte omfattet av regelverket

Husk databehandleravtale

- Databehandler direkte omfattet av regelverket
- Vær bevisst ved valg av databehandler
- Bruk databehandler som etterlever regelverket

Avvikshåndtering og rapportering

Alle får krav til avvikshåndtering- og rapportering

Avvik meldes til Datatilsynet uten ugrunnet opphold og senest innen 72 timer

- Innhold i avviksmeldingen
- Varsling av registrerte ved sikkerhetsbrudd

- Flere må ha personvernrådgiver

Nærmere om internkontroll

- Bedrifter vil få krav om å dokumentere virksomhetens internkontroll for hhv:
  - Personopplysninger
  - Datasikkerhet
- Må ha rutiner for å imøtekomme henvendelser om innsyn i personopplysninger
- Rutiner for sletting
- Rutiner for hva som skal gjøres dersom data kommer på avveie

Plikt til å gjøre en risikovurdering – personvernkonsekvenser?

- Plikt til å gjøre en risikovurdering før man iverksetter nye tiltak
- Hvis tiltak utgjør et stort inngrep i personvernet skal personvernkonsekvenser vurderes
- Hvis konklusjon: Høy personvernrisiko, og bedriften ikke kan redusere tiltaket selv, da starte forhåndsdrøftinger med Datatilsynet som gir råd og veiledning

MALER FRA ARBINN

Arbinn.no - https://arbinn.nho.no/forretningsdrift/personvern/personopplysningsverktoy/innforing/